24th ICCRTS

"Managing Cyber Risk to Mission"

Data is the key to Cyber Risk to Mission

Topic 1: Cyber Risk to Mission

Mr. Ken D. Teske

Mr. Mark E. Miller

Mr. Patrick J. Guerin

Mr. Gregory Robinson

Mr. Justin E. Schmidt

Mr. Robert Rosas

(Key Management Solutions)

Point of Contact

Ken D. Teske

Key Management Solutions

223 N Wahsatch Ave, STE 206

Colorado Springs, Colorado 80903-2253

(757) 510-0915 kteske@kmssecurity.com

Abstract

Managing Cyber Risk to Mission is the focus today, however for several decades Mission Partners, Coalitions, Alliances, Governments, Ministries, Departments, Bureaus, Agencies, Special Operations, and Conventional Forces have followed the constant changing focus on what the threat is to the “Mission”.

We may need to return to our roots to find the real source of the current Cyber Risk to Mission. We must analyze cyber security, information technology security, network security, computer security, physical security, insider threats, operational risk management, and data security to identify the real source to the cyber risk to mission. All of these focus areas over the past decades were intended to solve the risk to mission that was posed by each and everyone of the areas. We must look back at the starting point, data security. It’s all about the data.

We must use our collective best practices, approaches, strategies, and lessons learned to identify common goals, areas of interest, capabilities, and common categories of effort to gain the true Cyber risks, problems and issues. This understanding is the basis to addressing the risks to mission today and in the future.

Introduction

In order to have a common understanding of the real source of the current Cyber Risk to Mission, we may need to return to our roots to find the causes. We need to analyze cyber security, information technology security, network security, computer security, physical security, insider threats, operational risk management, and data security to identify the real source to the cyber risk to mission. Over the past decades, these focus areas were intended to solve the "risk to mission" that was posed by each and every one of the areas. We must look back at the starting point, data security, because in reality it's all about the data.

Let's start the analysis with a look at physical security that describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm such as espionage, theft, terrorist attacks, sabotage, damage, criminal activity and natural disasters. Physical security is often overlooked -- and its importance underestimated in favor of more technical threats such as hacking, malware, and cyberespionage. However, breaches of physical security can be carried out with brute force with little or no technical knowledge on the part of an attacker.

Physical security has three important components: access control, surveillance and testing. Obstacles should be placed in the way of potential attackers and physical sites should be hardened against accidents, attacks or environmental disasters. Such hardening measures include fencing, locks, access control cards, biometric access control systems and fire suppression systems. Second, physical locations should be monitored using surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors and smoke detectors. Third, disaster recovery policies and procedures should be updated and tested on a regular basis to achieve effective continuity of

operations and to reduce the time it takes to recover from disruptive man-made or natural disasters [A].

The internet of things (IoT) is widening the sphere of physical security as smart devices connected to our systems via the internet are located outside established secure perimeters. Isolating these smart devices can't be achieved in the same way as those within an organization's physical borders, so device location will play a key role in keeping equipment safe, secure and fully functional in the outside world.

As we examine the insider threat issue, we start with the term that is used to describe individuals with have access to information systems, who intentionally or unintentionally steal, damage, or expose an information system's data or infrastructure. Employees with access to an information system that are motivated by greed, grievances, or malicious intent fall into the intentional insider threat category. Employees who accidentally or inadvertently expose data or allow external threats to access a system fall into the unintentional insider threat category.

There are many factors that contribute to either type of insider threat. However, identifying the type of insider threat is a key component to understanding the motivations and underlying factors contributing to this type of threat. Some of these factors may include:

- Employee negligence
- Poor information system security practices, training programs and standards
- Poor, or a lack of security policies
- Personal problems for example: debt, drugs and alcohol, personality disputes
- Intellectual information sabotage

The threat from an insider has significantly increased over time and many organizations are implementing more stringent security practices and standards to reduce the ever-growing threat and consequence of this enormous risk to mission. Today's organizations place a high degree of faith and trust in their judgment and decisions. Many organizational leaders place trust in the individuals they hire to work on their information systems and these leaders also believe hired individuals have the organization's best interests in mind and will utilize the best information system's security behaviors and practices. At a certain point, this trust will be tested and, in some cases, broken due to an insider threat. An insider threat can be malicious or unintentional in nature, but either way it poses a risk to mission and jeopardizes the safety and security of organization employees. [C]

A computer security approach focuses on the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming more important due to increased reliance on computer systems, the Internet [D] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things" [C].

Still another approach identified previously is the network security approach which employs security 'layers' as part of wholistic, or Defense in Depth (DiD) approach to provide cyber risk to mission. DiD is an approach that employs a series of layered, defensive mechanisms and redundancies to protect valuable data and information as a whole. It addresses many different attack vectors because no organization can be ever be fully protected by a single layer of security. While it is interesting to note that each and every layer of and organization's security affects and is affected by other layers of security, the most important security objective of all layers is

ultimately to protect the user's data. One can discuss, define and implement security from an individual security layer perspective, multi-layer perspective, or wholistic DiD perspective, but the main objective of each of these perspectives is protection of data.

Another approach - information technology security focuses on techniques protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Major areas covered in information technology security are:

1) Application Security - Application security encompasses measures or countermeasures that are taken during the development lifecycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are input parameter validation, User/Role Authentication & Authorization, session management, parameter manipulation and exception management, and auditing and logging [D].

2) Information Security - Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are identification, authentication and authorization of user and cryptography [G].

3) Disaster recovery - Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in the event of a disaster. Every business should have a concrete disaster recovery plan to resume normal business operations as quickly as possible after a disaster [K].

4) Network Security - Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include a) Anti-

virus and anti-spyware, b) Firewall, to block unauthorized access to your network, c) Intrusion prevention [D].

The analysis of Operational Risk permeates all aspects of the risk spectrum throughout each and every organization whether it's a global corporation, a government agency or a small business and it overlaps with and all other types of risks within that organization such as cyber security, supply chain, procurement and normal operations. Operational Risk is a function of the complexity of the business and the environment the business operates in where loss is a consequence of critical contingencies which are generally quantitative in nature and are a result of operational failures outside of normal operations caused by unconscious execution errors or processing failures. Operational Risk in this context, are operational failures as a result of conscious violations of professional or moral standards and excessive risk taking that encompasses events with very differing frequencies and possibly patterns of occurrence and severities. Operational Risk is difficult to manage because it's not easy to develop a workable classification scheme or taxonomy for it. In order to manage operational risk through a structured process, it's important to have a mutually exclusive and exhaustive list of risk categories integrated into an Operational Risk Management framework. [J]

We still needed to look at ORM that is defined as: The risk of direct or indirect losses due to failures in systems, processes and people, or from external factors. Although this definition originated in the banking environment, it has been accepted as a generic definition by other enterprise sectors. Considering the key factors of Operational Risk and Operational Risk Management, it is evident that attempting to manage Operational Risk requires an enterprise level approach that encapsulates all aspects of the organization and begins to identify the quantitative data in order to accurately assess frequencies, patterns, severities and potential patterns leading up

to an organizational catastrophe. In today's operational environments, this requires operational risk not to be viewed as an afterthought, but as an integral part of the strategic planning, business management and enterprise risk management processes [E]. Another element to consider is how risk factors are interconnected to each other and to what degree. This approach warrants a systemic look at risk and it's impacts on the mission.

Now data security may be the real source to the cyber risk to mission. Data security is not the be all, end all for a security practice. It's one method of evaluating and reducing the risk that comes with storing any kind of data. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type.

Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers [F]. One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted [F].

The key elements of data security are confidentiality, integrity, and availability. Also known as the CIA triad, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration. Confidentiality ensures that data is accessed only by authorized individuals; Integrity ensures that information is reliable as well as

accurate; and Availability ensures that data is both available and accessible to satisfy business needs.

The last decade of IT management has seen a shift in the perception of data. Previously, having more data was almost always better than less. One can never be sure ahead of time what one might want to do with it. Today, data is a liability. The threat of a reputation-destroying data breach, loss in the millions or stiff regulatory fines all reinforce the thought that collecting anything beyond the minimum amount of sensitive data is extremely dangerous.

Conclusion

Since the inception of information technology, many mission-supporting security approaches have been proposed - each approach having its pros and cons. While some may try to compare one approach to another as being better or worse (or newer or older) as discussed in this paper, we believe that all approaches fundamentally focus on securing data. Rather than extrapolating that idea to say the ultimate, mission-supporting security approach is one approach such as data-centric security, we believe that cyber risk to mission is best mitigated when different approaches are employed to protect data. Essentially, employing numerous, overlapping approaches provides data "DiD'.

That said, there are ways to improve - via alignment and synchronization – the different, overlapping security approaches. A Cyber Risk to Mission Learning Environment needs to be created to share and learn lessons from all types of operations and units' experiences to address the challenges associated with working with different mission partners in any operation [H]. This learning environment will encourage stakeholders to engage and grow the environment into a holistic learning ecosystem enabling analysis, risk assessments, studies, new policies, provide technical advice and enable better recommendations. The environment will need to consider how

to store C2 and Cyber data and simplify access with next generation encryption that is quantum resistant and serves as an enabler for content delivery information through effective sharing, multi-domain aggerating from lowest to highest levels of protection, and the lexicons.

References

A. Rouse, M., (n.d.). Physical security. Retrieved from https://searchsecurity.techtarget.com/definition/physical-security

B. Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569

C. Cybersecurity Insiders. (2019). Ninety Percent of Organizations Are Vulnerable to Insider Threats According to New Cybersecurity Report. https://www.cybersecurity-insiders.com/ninety-percent-organizations-vulnerable-insider-threats-according-new-cybersecurity-report/

D. Warsinske, et al. (2019), The Official (ISC)2 Guide to the CISSP CBK Reference

E. Azvine, B., et al. "Operational risk management with real-time business intelligence." BT technology Journal 25.1 (2007): 154-167.

F. The rise of “big data” on cloud computing: Review and open research issues Information Systems, Volume 47, 2015, pp. 98-115 https://www.sciencedirect.com/science/article/pii/S1353485812700636

G. Varonis.2019. Michael Buckbee https://www.varonis.com/blog/data-security

H. Endsley, M. R., From here to autonomy: lessons learned from human–automation research. Human factors

I. Alberts, D., Garstka J., and Stein F., Network centric warfare. Developing and leveraging Information superiority

J. Muermann, Alexander, and Ulku Oktem. "The near-miss management of operational risk." The Journal of Risk Finance 4.1 (2002): 25-36. http://opim.wharton.upenn.edu/risk/downloads/02-02-MO.pdf

K. The Economic Times. 2019. Definition of cyber security https://economictimes.indiatimes.com/definition/cyber-security